

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Advanced Methods to Target and Eliminate)	CG Docket No. 17-59
Unlawful Robocalls)	

COMMENTS OF COMCAST CORPORATION

Matthew T. Murchison
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004

Kathryn A. Zachem
Beth A. Choroser
Regulatory Affairs

Francis M. Buono
Legal Regulatory

COMCAST CORPORATION
300 New Jersey Avenue, NW
Suite 700
Washington, DC 20001

Brian A. Rankin
Andrew D. Fisher
COMCAST CORPORATION
1701 JFK Boulevard
Philadelphia, PA 19103

September 24, 2018

TABLE OF CONTENTS

	Page
INTRODUCTION AND SUMMARY	1
DISCUSSION.....	3
I. THE COMMISSION SHOULD AUTHORIZE VOICE PROVIDERS TO USE ADDITIONAL OBJECTIVE CRITERIA TO IDENTIFY AND BLOCK ILLEGAL ROBOCALLS	3
A. The Commission Should Allow Voice Providers To Block Illegal Robocalls Identified Through SHAKEN/STIR.....	3
B. The Commission Should Permit Voice Providers To Block Illegal Robocalls Based on Traceback Findings	6
C. The Commission Also Should Pursue Policies That Promote the Responsible Use of Other Objective Criteria To Block Illegal Robocalls.....	8
D. Any New Rules Should Ensure That Voice Providers Retain Flexibility in Addressing Illegal Robocalls in Response to Such Objective Criteria.....	9
II. COMCAST CONTINUES TO SUPPORT EFFORTS TO ADDRESS ERRONEOUS BLOCKING OR LABELING OF LEGITIMATE CALLS	10
CONCLUSION.....	12

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Advanced Methods to Target and Eliminate)	CG Docket No. 17-59
Unlawful Robocalls)	

COMMENTS OF COMCAST CORPORATION

Comcast Corporation (“Comcast”) submits these comments in connection with the Public Notice issued on August 10, 2018 in the above-captioned proceeding.¹

INTRODUCTION AND SUMMARY

Comcast appreciates the opportunity to comment on the Consumer and Governmental Affairs Bureau’s latest Public Notice seeking to “refresh the record on how the Commission might further empower voice service providers to block illegal calls before they reach American consumers.”² The Commission already has made significant and laudable progress on this front, including by adopting an order last year authorizing voice providers to block calls appearing to originate from numbers on industry-maintained Do-Not-Originate (“DNO”) lists or from invalid, unallocated, or unassigned numbers.³ As is evident from recent submissions reporting on the progress made in combatting illegal robocalls, voice providers have already begun implementing

¹ *Consumer and Governmental Affairs Bureau Seeks to Refresh the Record on Advanced Methods to Target and Eliminate Unlawful Robocalls*, Public Notice, DA 18-842 (rel. Aug. 10, 2018) (“Public Notice”).

² *Id.* at 1.

³ *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706 ¶¶ 10, 18 (2017) (“*Robocall Blocking Order*”).

these Commission-authorized blocking techniques on their networks—with substantial success.⁴ These call-blocking techniques have provided an important additional layer of protection for consumers against abusive calling practices.

In light of these successes, the Commission should take this opportunity to expand the types of permissible robocall blocking techniques under its rules. More specifically, and as discussed further below, the Commission should adopt a rule expressly authorizing voice providers that have implemented the end-to-end call authentication protocol known as SHAKEN/STIR to block calls that fail authentication where the originating provider has also implemented that protocol for the type of call at issue. The Commission is already quite familiar with the development of this protocol and the great promise it holds for identifying illegal spoofed robocalls in a reliable manner, and plainly should allow voice providers to use this protocol to take action to protect consumers.

The Commission also should adopt a rule authorizing robocall blocking based on findings from industry traceback initiatives, and should consider ways to maximize participation in, and thereby the effectiveness of, traceback efforts. Additionally, because scammers’ tactics are constantly evolving, and because voice providers must constantly adapt their practices in response to these new tactics, the Commission should consider a more general rule authorizing voice providers to block calls based on any reasonable method recognized by industry standard-

⁴ See, e.g., Comments of Comcast Corp., CG Docket No. 17-59, at 4 (filed Jul. 20, 2018) (“Comcast Jul. 2018 Comments”) (describing “plans to begin deployment of a centralized capability for blocking calls appearing to originate from certain invalid and unallocated numbers,” which “will enable Comcast not only to block a significantly greater volume of fraudulent robocalls, but also to move quickly in adding or removing numbers or ranges of numbers to be blocked as appropriate”); Comments of AT&T Services, Inc., CG Docket No. 17-59, at 9 (filed Jul. 20, 2018) (“AT&T Jul. 2018 Comments”) (describing AT&T’s progress towards blocking calls appearing to originate from “invalid numbers”).

setting organizations or similar bodies—so that regulatory processes do not hold up the implementation of new robocall mitigation techniques developed by voice providers.

At the same time, voice providers should retain flexibility to address abusive calling activity in other ways, such as by labeling suspicious calls on device displays rather than blocking them outright. Comcast also supports efforts to minimize the number of false positives in any call-blocking or call-labeling approach, including through the creation of dedicated webpages for consumers and legitimate businesses to alert voice providers that their numbers are being incorrectly blocked or labeled. Taken together, these initiatives will build upon the successful advances that the Commission and industry participants have already made in combating illegal robocalls, and will expand the set of tools at voice providers' disposal for protecting their customers.

DISCUSSION

I. THE COMMISSION SHOULD AUTHORIZE VOICE PROVIDERS TO USE ADDITIONAL OBJECTIVE CRITERIA TO IDENTIFY AND BLOCK ILLEGAL ROBOCALLS

A. The Commission Should Allow Voice Providers To Block Illegal Robocalls Identified Through SHAKEN/STIR

The Public Notice appropriately revisits important questions from its *Robocall Blocking NPRM/NOI* on the sorts of objective criteria that voice providers could use to identify and block illegal robocalls. In particular, the Public Notice asks whether “providers [can] reliably identify calls that are highly likely to be illegal beyond those calls the Commission approved for blocking” in its *Robocall Blocking Order*, and, if so, “what criteria indicate that particular calls are illegal or warrant additional scrutiny methods providers can use to identify illegal calls.”⁵

⁵ Public Notice at 2.

One obvious example of an objective means for identifying fraudulent robocalls is the call authentication protocol known as SHAKEN (Signature-based Handling of Asserted Information Using toKENs) and STIR (Secure Telephone Identity Revisited). As Comcast and others have noted previously, SHAKEN/STIR currently represents the most promising way of addressing illegal spoofed robocalls in a comprehensive and robust manner.⁶ The STIR framework allows a provider to cryptographically sign, or attest to, calling party information at its origin and to verify this information at the call termination point; SHAKEN, in turn, defines a methodology for providers using STIR to communicate authentication information across networks.⁷ The Robocall Strike Force found that SHAKEN/STIR “holds considerable promise for repressing the presence of robocalling in the communications ecosystem,” as it will “provide a basis for verifying calls, classifying calls, and facilitating the ability to trust caller identity end to end.”⁸ Various voice providers are now in the process of developing and deploying SHAKEN/STIR on their networks.⁹

⁶ See Comments of Comcast Corp., CG Docket No. 17-59, at 6, 7, 11 (filed Jul. 3, 2017) (“Comcast Jul. 2017 Comments”); see also, e.g., Comments of CTIA, WC Docket No. 17-97, at 1 (filed Aug. 14, 2017) (noting that “[t]he SHAKEN/STIR framework developed by these standard-setting bodies has received widespread acclaim” and “is the appropriate framework for call authentication”); Comments of USTelecom, CG Docket No. 17-59, at 4 (filed Jul. 20, 2018) (noting that “there is strong industry commitment to the deployment of the SHAKEN and STIR standards,” which “should improve the reliability of the nation’s communications system by better identifying legitimate traffic”).

⁷ See Comcast Jul. 2017 Comments at 7.

⁸ See Robocall Strike Force, *Robocall Strike Force Report*, at 5 (rel. Oct. 26, 2016), available at <https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf> (“Oct. 2016 Strike Force Report”).

⁹ See, e.g., Comcast Jul. 2018 Comments at 3-4 (explaining that, in addition to leading efforts to develop standards and a governance framework for SHAKEN/STIR, “Comcast has been actively participating in SHAKEN/STIR testbeds along with other voice providers, and plans to conduct network trials of SHAKEN/STIR prior to the end of 2018”).

Given the pending implementation of SHAKEN/STIR, the Commission should adopt a rule expressly authorizing voice providers to block unauthenticated calls where authentication fails and the originating and terminating providers have implemented SHAKEN/STIR for the type of call at issue.¹⁰ Adopting such a rule not only would clearly enable voice providers that have implemented SHAKEN/STIR to use that reliable protocol to block harmful calls, but also would encourage other providers to implement SHAKEN/STIR, thus further mitigating the rise of abusive call rates.¹¹ Such a rule also would not lead to a significant number of “false positives” in blocking calls; the SHAKEN/STIR framework already enables voice providers to distinguish fraudulently spoofed calls from calls where the caller ID information has been changed for legitimate reasons, and allows for “partial attestation” of the call in that latter context in a manner that would signal that the call is legitimate.¹² Moreover, by limiting permissible blocking to calls that fail authentication where SHAKEN/STIR has been implemented by *both* the originating provider and terminating provider for the type of call at issue, such a rule would avoid authorizing blocking where the lack of authentication is caused by one provider’s failure to implement the protocol in whole or in part.

and scale to fuller implementation during 2019”); AT&T Jul. 2018 Comments at 6 (committing to “begin authenticating calls in 2019” under the SHAKEN/STIR framework); Comments of Verizon, CG Docket No. 17-59, at 6 (filed Jul. 20, 2018) (reporting that Verizon “expect[s] to achieve initial operational capability with STIR/SHAKEN this year, with the bulk of production coming on line in 2019”).

¹⁰ Comcast Jul. 2017 Comments at 9. However, this proposed rule would not authorize blocking where at least one of the providers transmitting the call has not implemented SHAKEN/STIR for the type of call at issue.

¹¹ *Id.*

¹² *See* Oct. 2016 Strike Force Report at 9.

B. The Commission Should Permit Voice Providers To Block Illegal Robocalls Based on Traceback Findings

In exploring other possible “objective criteria” that could guide efforts to address illegal robocalls, the Public Notice asks whether information gained through traceback efforts could enable “providers [to] . . . stop [unlawful robocalls] from reaching customers in the future.”¹³ The Commission posed a similar question in its 2017 *Robocall Blocking NPRM/NOI*, asking whether “information obtained through traceback efforts is, can, and should be used to identify future calls that are illegal to a reasonably high degree of certainty.”¹⁴

In Comcast’s experience, traceback initiatives, when undertaken with the full cooperation of all providers along a call path, can often result in the clear identification of originating numbers being used for fraudulent calling. The Robocall Strike Force found the same in its report—noting that, in recent trials, “the sharing of certain network intelligence and traceback information among [the] participants . . . did lead to the successful thwarting and mitigation of unwanted and illegal phone traffic.”¹⁵ Comcast has been an active participant in these joint traceback efforts, including through its participation in the USTelecom Traceback Group.¹⁶ In light of the positive impact of these collaborative efforts, Comcast has consistently supported—and continues to support—a rule authorizing voice providers to block calls that, based on

¹³ Public Notice at 2-3.

¹⁴ *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Noticed of Proposed Rulemaking and Notice of Inquiry, 32 FCC Rcd 2306 ¶ 30 (2017) (“*Robocall Blocking NPRM/NOI*”).

¹⁵ See Robocall Strike Force, *Industry Robocall Strike Force Report*, at 1 (rel. Apr. 28, 2017), available at <https://www.fcc.gov/file/12311/download> (“Apr. 2017 Strike Force Report”).

¹⁶ See Public Notice at 3 (asking “[w]hich providers are participating in the USTelecom Traceback Group”).

information obtained through tracebacks, are determined with a reasonably high degree of certainty to be illegal spoofed robocalls.¹⁷

The Commission also should take affirmative steps to encourage all carriers to participate fully in traceback initiatives in order to make this method for addressing illegal robocalls as robust as possible. To be sure, the advent of SHAKEN/STIR likely will streamline the traceback process significantly;¹⁸ as the Robocall Strike Force has noted, the SHAKEN protocol “has defined a unique Originating Identifier (origid) which has been specifically incorporated to make traceback an easy and automatic process, specifically identifying[,] beyond the service provider that originated the call, the specific service provider customer or gateway node” associated with the call.¹⁹ However, until SHAKEN/STIR is widely deployed, traceback initiatives will continue to be “cumbersome in terms of manual investigation of call logs hop by hop.”²⁰ And “while numerous providers have formally joined [industry] traceback efforts, and many others cooperate in good faith in tracebacks, there are still upstream carriers who refuse to cooperate, which prevents carriers from tracing these malicious calling events back to the origin of the call.”²¹ The Commission thus should consider ways to foster greater participation in traceback efforts by all retail voice providers and intermediate carriers—e.g., by adopting a safe harbor from any traceback-related reporting requirements for entities that certify to the Commission that they

¹⁷ See Comcast Jul. 2017 Comments at 16.

¹⁸ See Public Notice at 3 (seeking comment on “[h]ow . . . SHAKEN/STIR [will] affect traceback”).

¹⁹ Oct. 2016 Strike Force Report at 9-10.

²⁰ *Id.* at 9.

²¹ Apr. 2017 Strike Force Report at 19.

participate in traceback efforts—to ensure that these efforts continue to bear fruit and provide a solid foundation for blocking by voice providers going forward.²²

C. The Commission Also Should Pursue Policies That Promote the Responsible Use of Other Objective Criteria To Block Illegal Robocalls

In addition to specifically authorizing blocking based on the use of SHAKEN/STIR protocols and on information obtained through traceback initiatives, the Commission should strongly consider adopting a tailored rule that authorizes voice providers to block calls determined to be illegal spoofed robocalls using any reasonable and proven method affirmatively approved by industry standard-setting organizations or similar bodies.

Doing so would ensure that regulatory processes do not hamper the development and implementation of such criteria to protect consumers. The Commission has correctly observed that “illegitimate callers us[e] evolving methods to continue making illegal robocalls” and seek to circumvent the protections that voice providers put in place.²³ Voice providers, in turn, are constantly innovating and working together to develop new methods to stay one step ahead of illegitimate callers. Voice providers need the flexibility to take action against abusive calling without the need to wait for regulatory approval every time a new fraudulent practice is invented.

As Comcast has noted in the past, if the Commission believes it is necessary to engage in some review of future methods for addressing illegal spoofed robocalls, it should do so in a way that minimizes delays and avoids disclosing sensitive details of these methods to illegitimate callers.²⁴ One potential method could be to establish an expedited process with a clear and

²² See Public Notice at 3 (asking whether “there [are] any other concerns that the Commission could address to facilitate traceback”).

²³ *Robocall Blocking NPRM/NOI* ¶ 6.

²⁴ See Comcast Jul. 2017 Comments at 17 n.61.

predictable timeline in which the Commission can review and bless blocking methods on a confidential basis.²⁵ Whatever the process, however, the Commission should ensure that voice providers are not hamstrung in their efforts to adapt to the evolving practices of bad actors and to prevent circumvention of voice providers' techniques for mitigating illegal spoofed robocalls.

D. Any New Rules Should Ensure That Voice Providers Retain Flexibility in Addressing Illegal Robocalls in Response to Such Objective Criteria

In authorizing voice providers to block illegal robocalls in these additional circumstances, the Commission should be careful not to *mandate* blocking in every instance, and instead should ensure that voice providers continue to have flexibility to take appropriate action in response to calls identified through these objective criteria. Notably, the practice of “labeling” calls as suspicious is entirely consistent with industry standards for identifying and addressing illegal robocalls.²⁶ Indeed, the SHAKEN/STIR protocol does not itself dictate how a voice provider must address an unauthenticated call, and leaves it to the voice provider to decide whether to block the call, label the call as suspicious, or take no action. Moreover, as the Public Notice correctly points out, some voice providers already make available third-party applications that can label calls as suspicious on consumer devices rather than blocking those calls outright.²⁷ In continuing to deploy these robocall identification techniques, voice providers may well find that consumers prefer a call-labeling approach in some circumstances and a call-blocking approach in others.

²⁵ *See id.*

²⁶ *See* Public Notice at 2-3.

²⁷ *See id.* (discussing the practice of “call labeling” and noting that “[t]here are numerous third-party applications that offer . . . labeling services directly to consumers”).

Accordingly, at this stage, the Commission should refrain from mandating blocking in all instances, and instead frame its rules as *permitting* blocking alongside other approaches for identifying and addressing these calls. This approach would be consistent with the one taken in last year’s *Robocall Blocking Order*—which similarly permitted rather than mandated blocking for calls appearing to originate from numbers on industry DNO lists or from invalid, unallocated, or unassigned numbers.²⁸ A permissive approach not only would give voice providers sufficient flexibility to respond to threats while accounting for evolving consumer preferences, but also would alleviate any concerns regarding the potential costs to small voice providers associated with implementing new call blocking technologies on their networks.²⁹

II. COMCAST CONTINUES TO SUPPORT EFFORTS TO ADDRESS ERRONEOUS BLOCKING OR LABELING OF LEGITIMATE CALLS

Finally, the Public Notice asks how to “reduce the potential for false positives” and “how to address situations in which false positives occur.”³⁰ As noted above and in other filings in this proceeding, Comcast believes that the incidence of false positives will continue to be relatively

²⁸ See *Robocall Blocking Order* ¶¶ 10, 19, 23, 27, 39. Moreover, consistent with that *Order*, the Commission should again clarify that any new rules authorizing blocking “do not require consumer opt-in” before a provider may engage in such blocking. *Id.* ¶ 7.

²⁹ See *id.*, App’x C, ¶ 33 (explaining that the *Robocall Blocking Order* “implemented permissive rules to address the concerns of voice service providers, including small businesses, that the cost and burden of complying with mandatory rules could be significant and might require implementation of new technology”).

³⁰ Public Notice at 3. The Commission should remain wary of relying too heavily on the use of “white lists” to minimize the erroneous blocking of legitimate calls. See *id.* at 4. For example, vendors administering such lists should be prohibited from charging consumers or businesses to have their numbers added to a white list (or, alternatively, to have their numbers removed from a black list). Plainly, one’s ability to pay should not be a valid criterion for adding or removing one’s number to or from these lists; indeed, payment requirements risk undermining the accuracy of these lists by interfering with otherwise valid requests to add or remove numbers.

low, not only under the Commission’s existing call blocking rules but also under the further rules proposed herein. For instance, the SHAKEN/STIR framework already includes mechanisms for eliminating false positives—including by allowing for “partial attestation” of a call where caller ID information has been changed for legitimate reasons (rather than leaving such calls entirely unauthenticated, which might otherwise lead to false positives).³¹

At the same time, Comcast supports further efforts to remedy situations where calls originating from a consumer or a legitimate business are being blocked or labeled incorrectly. As Comcast has explained previously, the Commission could consider adopting a rule “requiring all voice providers to establish their own easy-to-find web pages enabling individuals and entities to report erroneous blocking” or labeling.³² Comcast continues to believe that this approach would prove highly effective at addressing any erroneous blocking or labeling, as voice providers have strong market-driven incentives to address any erroneous blocking or labeling as soon as they become aware of the issue.³³ Such an approach also would obviate any need for the Commission to impose a one-size-fits-all challenge mechanism.³⁴ And to the extent that voice providers rely on third-party vendors to manage their robocall mitigation tools, the Commission should take steps to encourage efficient remediation of any erroneous blocking or labeling by those vendors as well—including by specifying that voice providers’ web pages include contact information for those vendors, so that the entity that is best positioned to take remedial action can do so promptly and efficiently.

³¹ See *supra* at 5.

³² Comments of Comcast Corp., CG Docket No. 17-59, at 4, 5 (filed Jan. 23, 2018).

³³ See *id.* at 4.

³⁴ See *id.* at 4-5.

CONCLUSION

Comcast appreciates the Commission's continued focus on the problem of unlawful robocalls. The Commission has already made significant strides towards empowering voice providers to tackle this problem, and the proposals discussed above and in the Public Notice represent a natural next step in the effort to protect consumers from these abusive practices.

Respectfully submitted,

/s/ Kathryn A. Zachem

Matthew T. Murchison
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004

Kathryn A. Zachem
Beth A. Choroser
Regulatory Affairs

Francis M. Buono
Legal Regulatory

COMCAST CORPORATION
300 New Jersey Avenue, NW
Suite 700
Washington, DC 20001

Brian A. Rankin
Andrew D. Fisher
COMCAST CORPORATION
1701 JFK Boulevard
Philadelphia, PA 19103

September 24, 2018